

In the Claims:

This listing of claims will replace all prior versions and listings of claims in the application.

- 1 1-5. (canceled).
- 1 6. (currently amended) The method of claim [[1]] 76, wherein producing an array of session  
2 random encryption [[key]] keys at the first station includes:
  - 3 providing a buffer at the first station;
  - 4 generating said keys and storing said keys in the buffer;
  - 5 associating respective session random key initiation intervals with said keys stored in said  
6 buffer;
  - 7 [[using]] selecting keys from said buffer as said selected session random symmetric  
8 encryption key [[keys]] in response to corresponding requests received by said first station  
9 during said respective session random key initiation intervals ~~for use in a first exchange of said~~  
10 ~~plurality of exchanges~~;
  - 11 removing keys from said buffer after expiry of [[the]] respective session random key  
12 lifetimes, where the session random key lifetimes expire after the session random symmetric  
13 encryption key initiation intervals lifetime in the buffer.
- 1 7. (original) The method of claim 6, wherein said buffer is managed as a circular buffer.
- 1 8. (original) The method of claim 6, wherein a session random key lifetime in the buffer for said  
2 plurality of exchanges has a value within which the plurality of exchanges can be completed in  
3 expected circumstances, and said keys are removed from said buffer after a multiple M times  
4 said value of session random key lifetime to engage into establishing a communication session,  
5 where M is less than or equal to 10.
- 1 9. (currently amended) The method of claim 6, wherein a session random key lifetime in the  
2 buffer for said plurality of exchanges has a value within which the plurality of exchanges can be  
3 completed in expected circumstances, and said keys are removed from said buffer after a

4       multiple M times said value, and the session random key lifetime to engage into establishing a  
5       communication session is less than about 90 second seconds.

1       10. (canceled).

1       11. (currently amended) The method of claim [[1]] 76, wherein producing an encryption key at  
2       the first station includes:

3       — assigning, in said first station, a session random key for use within a session random key  
4       initiation interval in response to requests received by said first station during said session random  
5       key initiation interval for use in a first exchange of said plurality of exchanges;

6       — associating, in said first station, a plurality of intermediate data random keys with said  
7       request for use in said plurality of exchanges;

8               wherein said plurality of exchanges includes

9               a first exchange including sending a first message from the first station carrying said  
10               selected session random symmetric encryption key to the second station, where  
11               the second station returns a second message carrying a shared parameter the  
12               identifier of the second station encrypted using [[the]] said selected session  
13               random symmetric encryption key, and decrypting the shared parameter identifier  
14               of the second station at the first station to validate the second station, or a user at  
15               the second station; and

16               a second exchange including sending a further message from the first station to the  
17               second station, the further message carrying a particular data random symmetric  
18               encryption key from said sub-array plurality of intermediate data random keys  
19               encrypted using [[the]] said selected session random symmetric encryption key,  
20               where the second station returns another message carrying a hashed version of  
21               said particular data random symmetric key encrypted using said particular  
22               enryptiondata random symmetric key to the first station, and decrypting said  
23               hashed version of said particular data random symmetric key at the first station  
24               using said particular data random symmetric key.

1       12. (currently amended) The method of claim [[1]] 76, including wherein producing an  
2 encyption key at the first station includes:  
3       assigning, in said first station, a session random key for use within a session random key  
4 initiation interval in response to requests received by said first station during said session random  
5 key initiation interval for use in a first exchange of said plurality of exchanges;  
6       associating, in said first station, a plurality of intermediate data random keys with said  
7 request for use in said plurality of exchanges; and

8               after said request for initiation of a communication session, presenting to the second  
9 station a user interface along with [[the]] said selected session random symmetric encryption  
10 key, said user interface including a prompt for entry of said identifier of the second station a  
11 shared parameter and at least one of said first and second shared secrets secret.

1       13. (currently amended) The method of claim [[1]] 76, including wherein producing an  
2 encyption key at the first station includes:  
3       assigning, in said first station, a session random key for use within a session random key  
4 initiation interval in response to requests received by said first station during said session random  
5 key initiation interval for use in a first exchange of said plurality of exchanges;  
6       associating, in said first station, a plurality of intermediate data random keys with said  
7 request for use in said plurality of exchanges; and

8               after said request for initiation of a communication session, presenting to the second  
9 station a user interface along with the session random key, said user interface including a prompt  
10 for entry of said identifier of the second station a shared parameter and said first and second at  
11 least two shared secrets.

1       14. (currently amended) The method of claim [[1]] 11, including wherein producing an  
2 encyption key at the first station includes:  
3       assigning, in said first station, a session random key for use within a session random key  
4 initiation interval in response to requests received by said first station during said session random  
5 key initiation interval for use in a first exchange of said plurality of exchanges;  
6       associating, in said first station, a plurality of intermediate data random keys with said  
7 request for use in said plurality of exchanges;

8       — wherein said plurality of exchanges includes  
9            a first exchange including sending a first message from the first station carrying said  
10          session random key to the second station, where the second station returns a  
11          second message carrying a shared parameter encrypted using the session random  
12          key, and decrypting the shared parameter at the first station; and—  
13          a second exchange including sending a third message from the first station to the second  
14          station, the third message carrying a particular data random key from said  
15          plurality of intermediate data random keys encrypted using the session random  
16          key, where the second station returns a fourth message carrying a hashed version  
17          of said particular data random key encrypted using said particular data random  
18          key to the first station, and decrypting said hashed version of said particular data  
19          random key at the first station using said particular data random key;  
20          and then executing at least one additional exchange in said plurality of exchanges,  
21          where

22            said at least one additional exchange includes sending an additional message from the  
23          first station to the second station carrying a next data random symmetric key from  
24          said sub-array the plurality of intermediate data random keys associated with said  
25          request, encrypted using a data random symmetric key from said sub-array  
26          exchanged during a previously completed exchange in said plurality of  
27          exchanges, where the second station decrypts said next data random symmetric  
28          key and returns a responsive message carrying a hashed version of said next data  
29          random symmetric key encrypted using said next data random symmetric key, and  
30          decrypting at the first station said hashed version of said next data random  
31          symmetric key using said next data random symmetric key.

1       15. (canceled).

1       16. (original) The method of claim 14, including executing more than one of said additional  
2          exchanges.

1       17-21. (canceled).

1    22. (currently amended) The method of claim 76 [[17]], including upon request for initiation of a  
2    communication session, presenting to the second station a user interface for initiation of an  
3    authentication session including a compiled version of [[the]] said selected session random  
4    symmetric encryption key and parameters for one or more conversion arrays, said user interface  
5    including a prompt for entry of the said identifier of the second station shared parameter and at  
6    least one of said first and second shared secrets secret.

1    23-24. (canceled).

1    25. (currently amended) The method of claim [[14]] 76, including ~~executing a further exchange~~  
2    ~~including~~

3         ~~sending a message from the first station to the second station carrying said encryption key~~  
4         ~~encrypted using a first shared secret to the second station, where the second~~  
5         ~~station returns a message carrying a hashed version of said encryption key~~  
6         ~~encrypted using said first shared secret, and decrypting said encryption key at the~~  
7         ~~first station;~~

8         ~~sending a message from the first station to the second station carrying said encryption key~~  
9         ~~encrypted using a second shared secret, where the second station decrypts said~~  
10        ~~encryption key, and returns a message to the first station carrying a hashed~~  
11        ~~version of the encryption key encrypted using said second shared secret; and~~  
12        sending a message from the first station to the second station carrying an authentication  
13        signal indicating success or failure of mutual authentication and establishment of  
14        the final symmetric encryption key, said authentication signal being encrypted  
15        using one of said intermediate data random symmetric keys from a previous  
16        exchange in the plurality of exchanges.

1    26-30. (canceled).

1    31. (currently amended) The apparatus of claim [[26]] 77, wherein said logic to produce an array  
2    of session random symmetric encryption keys provide ephemeral encryption keys at the first  
3    station includes instructions:

4           providing a buffer at the first station;  
5           generating said keys and storing said keys in the buffer;  
6           associating respective session random key initiation intervals with said keys stored in said  
7 buffer;  
8           [[using]] selecting keys from said buffer as said selected session random symmetric  
9 encryption keys in response to requests received by said first station during said respective  
10 session random key initiation intervals ~~for use in a first exchange of said plurality of exchanges;~~  
11           removing keys from said buffer after expiry of the respective session random key  
12 lifetimes, where the session random key lifetimes expire after the session random key initiation  
13 intervals lifetime in the buffer.

1       32. (original) The apparatus of claim 31, wherein said buffer is managed as a circular buffer.

1       33. (currently amended) The apparatus of claim 31, wherein a session random key lifetime in the  
2 buffer for said plurality of exchanges has a value within which the plurality of exchanges can be  
3 completed in expected circumstances, and said keys are removed from said buffer after a  
4 multiple M times said value ~~session random key lifetime~~ to engage into establishing a  
5 communication session, where M is less than or equal to 10.

1       34. (currently amended) The apparatus of claim 31, wherein a session random key lifetime in the  
2 buffer for said plurality of exchanges has a value within which the plurality of exchanges can be  
3 completed in expected circumstances, and said keys are removed from said buffer after a  
4 multiple M times said value ~~session random key lifetime~~ to engage into establishing a  
5 communication session, and the session random key lifetime to engage into establishing a  
6 communication session is less than about 90 seconds ~~second~~.

1       35. (canceled).

1       36. (currently amended) The apparatus of claim [[26]] 77, wherein said logic to provide  
2 ephemeral encryption keys at the first station includes instructions:

3       assigning, in said first station, a session random key for use within a session random key  
4 initiation interval in response to requests received by said first station during said session random  
5 key initiation interval for use in a first exchange of said plurality of exchanges;

6       associating, in said first station, a plurality of intermediate data random keys with said  
7 request for use in said plurality of exchanges;

8           wherein said plurality of exchanges includes

9           a first exchange including sending a first message from the first station carrying said  
10           selected session random symmetric encryption key to the second station, where  
11           the second station returns a second message carrying said identifier of the second  
12           station a shared parameter encrypted using [[the]] said selected session random  
13           symmetric encryption key, and decrypting said identifier of the second station the  
14           shared parameter at the first station to validate the second station; and

15           a second exchange including sending a further message from the first station to the  
16           second station, the further message carrying a particular data random symmetric  
17           key from said sub-array plurality of intermediate data random keys encrypted  
18           using [[the]] said selected session random key, where the second station returns  
19           another message carrying a hashed version of said particular data random  
20           symmetric key encrypted using said particular encryption-data random symmetric  
21           key to the first station, and decrypting said hashed version of said particular data  
22           random symmetric key at the first station using said particular data random  
23           symmetric key.

1       37. (currently amended) The apparatus of claim [[26]] 77, wherein said logic to provide  
2       ephemeral encryption keys at the first station includes instructions:

3       assigning, in said first station, a session random key for use within a session random key  
4 initiation interval in response to requests received by said first station during said session random  
5 key initiation interval for use in a first exchange of said plurality of exchanges;

6       associating, in said first station, a plurality of intermediate data random keys with said  
7 request for use in said plurality of exchanges; and

8           logic to present, after said request for initiation of a communication session, presenting to  
9 the second station a user interface along with the selected session random symmetric encryption

10 key, said user interface including a prompt for entry of said identifier of the second station a  
11 shared parameter and at least one of said first and second shared secrets secret.

1 38. (currently amended) The apparatus of claim [[26]] 77, ~~wherein said logic to provide~~  
2 ~~ephemeral encryption keys at the first station includes instructions:~~  
3 ~~— assigning, in said first station, a session random key for use within a session random key~~  
4 ~~initiation interval in response to requests received by said first station during said session random~~  
5 ~~key initiation interval for use in a first exchange of said plurality of exchanges;~~  
6 ~~— associating, in said first station, a plurality of intermediate data random keys with said~~  
7 ~~request for use in said plurality of exchanges; and~~  
8 ~~logic to present, after said request for initiation of a communication session, presenting to~~  
9 ~~the second station a user interface along with the selected session random symmetric encryption~~  
10 ~~key, said user interface including a prompt for entry of said identifier of the second station a~~  
11 ~~shared parameter and at least two said first and second shared secrets.~~

1 39. (currently amended) The apparatus of claim [[26]] 36, ~~wherein said logic to provide~~  
2 ~~ephemeral encryption keys at the first station includes instructions:~~  
3 ~~— assigning, in said first station, a session random key for use within a session random key~~  
4 ~~initiation interval in response to requests received by said first station during said session random~~  
5 ~~key initiation interval for use in a first exchange of said plurality of exchanges;~~  
6 ~~— associating, in said first station, a plurality of intermediate data random keys with said~~  
7 ~~request for use in said plurality of exchanges;~~  
8 wherein said plurality of exchanges includes  
9 ~~a first exchange including sending a first message from the first station carrying said~~  
10 ~~session random key to the second station, where the second station returns a~~  
11 ~~second message carrying a shared parameter encrypted using the session random~~  
12 ~~key, and decrypting the shared parameter at the first station; and~~  
13 ~~a second exchange including sending a third message from the first station to the second~~  
14 ~~station, the third message carrying a particular data random key from said~~  
15 ~~plurality of intermediate data random keys encrypted using the session random~~  
16 ~~key, where the second station returns a fourth message carrying a hashed version~~

17           ~~of said particular data random key encrypted using said particular data random~~  
18           ~~key to the first station, and decrypting said hashed version of said particular data~~  
19           ~~random key at the first station using said particular data random key;~~  
20           ~~and then executing~~ at least one additional exchange in said plurality of exchanges,  
21 where

22           said at least one additional exchange includes sending an additional message from the  
23           first station to the second station carrying a next data random symmetric key from  
24           said sub-array~~the plurality of intermediate data random keys associated with said~~  
25           request, encrypted using a data random symmetric key from said sub-array  
26           exchanged during a previously completed exchange in said plurality of  
27           exchanges, where the second station decrypts said next data random symmetric  
28           key and returns a responsive message carrying a hashed version of said next data  
29           random symmetric key encrypted using said next data random symmetric key, and  
30           decrypting at the first station said hashed version of said next data random  
31           symmetric key using said next data random symmetric key.

1       40. (canceled).

1       41. (original) The apparatus of claim 39, including logic executing more than one of said  
2       additional exchanges.

1       42-46. (canceled).

1       47. (currently amended) The apparatus of claim 77 [[42]], including upon request for initiation of  
2       a communication session, logic to present to the second station a user interface for initiation of  
3       an authentication session including a compiled version of the session random symmetric  
4       encryption key and parameters for one or more conversion arrays, said user interface including a  
5       prompt for entry of said identifier of the second station the shared parameter, and at least one of  
6       said first and second shared secrets secret.

1       48-49. (canceled).

1    50. (currently amended) The apparatus of claim [[39]] 77, including logic executing a further  
2    exchange including instructions

3                 ~~sending a message from the first station to the second station carrying said encryption key~~  
4                 ~~encrypted using a first shared secret to the second station, where the second~~  
5                 ~~station returns a message carrying a hashed version of said encryption key~~  
6                 ~~encrypted using said first shared secret, and decrypting said encryption key at the~~  
7                 ~~first station;~~

8                 ~~sending a message from the first station to the second station carrying said encryption key~~  
9                 ~~encrypted using a second shared secret, where the second station decrypts said~~  
10                ~~encryption key, and returns a message to the first station carrying a hashed~~  
11                ~~version of the encryption key encrypted using said second shared secret; and~~  
12                sending a message from the first station to the second station carrying an authentication  
13                signal indicating success or failure of mutual authentication and establishment of  
14                the final symmetric encryption key, said authentication signal being encrypted  
15                using one of said intermediate data random symmetric keys from a previous  
16                exchange in the plurality of exchanges.

1    51-55. (canceled).

1    56. (currently amended) The article of claim 78 [[51]], wherein said logic to produce an array of  
2    session random symmetric encryption keys ~~provide ephemeral encryption~~ keys at the first  
3    station includes instructions:

4                 providing a buffer at the first station;

5                 generating said keys and storing said keys in the buffer;

6                 associating respective session random key initiation intervals with said keys stored in said  
7    buffer;

8                 ~~[[using]] selecting keys from said buffer as said selected session random symmetric~~

9                 ~~encryption keys in response to requests received by said first station during said respective~~

10                ~~session random key initiation intervals for use in a first exchange of said plurality of exchanges;~~

11           removing keys from said buffer after expiry of the respective session random key  
12 lifetimes, where the session random key lifetimes expire after the session random key initiation  
13 intervals lifetime in the buffer.

1       57. (original) The article of claim 56, wherein said buffer is managed as a circular buffer.

1       58. (currently amended) The article of claim 56, wherein a session random key lifetime in the  
2       buffer for said plurality of exchanges has a value within which the plurality of exchanges can be  
3       completed in expected circumstances, and said keys are removed from said buffer after a  
4       multiple M times said value ~~of session random key lifetime~~ to engage into establishing a  
5       communication session, where M is less than or equal to 10.

1       59. (original) The article of claim 56, wherein a session random key lifetime in the buffer for  
2       said plurality of exchanges has a value within which the plurality of exchanges can be completed  
3       in expected circumstances, and said keys are removed from said buffer after a multiple M times  
4       said value, and the session random key lifetime to engage into establishing a communication  
5       session is less than about 90 seconds.

1       60. (canceled).

1       61. (currently amended) The article of claim 78 [[51]], ~~wherein said logic to provide ephemeral~~  
2       ~~encryption keys at the first station includes instructions:~~

3       ~~assigning, in said first station, a session random key for use within a session random key~~  
4       ~~initiation interval in response to requests received by said first station during said session random~~  
5       ~~key initiation interval for use in a first exchange of said plurality of exchanges;~~  
6       ~~associating, in said first station, a plurality of intermediate data random keys with said~~  
7       ~~request for use in said plurality of exchanges;~~

8           wherein said plurality of exchanges includes

9           a first exchange including sending a first message from the first station carrying said  
10          selected session random symmetric encryption key to the second station, where  
11          the second station returns a second message carrying said identifier of the second

12           station a shared parameter encrypted using [[the]] said selected session random  
13           symmetric encryption key, and decrypting said identifier of the second station the  
14           shared parameter at the first station to validate the second station; and  
15           a second exchange including sending a further message from the first station to the  
16           second station, the further message carrying a particular data random symmetric  
17           key from said sub-array plurality of intermediate data random keys encrypted  
18           using [[the]] said selected session random key, where the second station returns  
19           another message carrying a hashed version of said particular data random  
20           symmetric key encrypted using said particular encryption-data random symmetric  
21           key to the first station, and decrypting said hashed version of said particular data  
22           random symmetric key at the first station using said particular data random  
23           symmetric key.

1       62. (currently amended) The article of claim 78 [[51]], wherein said logic to provide ephemeral  
2       encryption keys at the first station includes instructions:

3        assigning, in said first station, a session random key for use within a session random key  
4       initiation interval in response to requests received by said first station during said session random  
5       key initiation interval for use in a first exchange of said plurality of exchanges;  
6        associating, in said first station, a plurality of intermediate data random keys with said  
7       request for use in said plurality of exchanges; and

8        logic to present, after said request for initiation of a communication session, presenting to  
9       the second station a user interface along with the selected session random symmetric encryption  
10      key, said user interface including a prompt for entry of said identifier of the second station a  
11      shared parameter and at least one of said first and second shared secrets secret.

1       63. (currently amended) The article of claim 78 [[51]], wherein said logic to provide ephemeral  
2       encryption keys at the first station includes instructions:

3        assigning, in said first station, a session random key for use within a session random key  
4       initiation interval in response to requests received by said first station during said session random  
5       key initiation interval for use in a first exchange of said plurality of exchanges;

6 ————— associating, in said first station, a plurality of intermediate data random keys with said  
7 request for use in said plurality of exchanges; and

8       logic to present, after said request for initiation of a communication session, presenting to  
9 the second station a user interface along with the selected session random symmetric encryption  
10 key, said user interface including a prompt for entry of said identifier of the second station a  
11 shared parameter and at least two said first and second shared secrets.

1 64. (currently amended) The article of claim 61 [[51]], wherein said logic to provide ephemeral  
2 encryption keys at the first station includes instructions:

3 ————— assigning, in said first station, a session random key for use within a session random key  
4 initiation interval in response to requests received by said first station during said session random  
5 key initiation interval for use in a first exchange of said plurality of exchanges;

6 ————— associating, in said first station, a plurality of intermediate data random keys with said  
7 request for use in said plurality of exchanges;

8       wherein said plurality of exchanges includes

9       a first exchange including sending a first message from the first station carrying said  
10 session random key to the second station, where the second station returns a  
11 second message carrying a shared parameter encrypted using the session random  
12 key, and decrypting the shared parameter at the first station; and

13       a second exchange including sending a third message from the first station to the second  
14 station, the third message carrying a particular data random key from said  
15 plurality of intermediate data random keys encrypted using the session random  
16 key, where the second station returns a fourth message carrying a hashed version  
17 of said particular data random key encrypted using said particular data random  
18 key to the first station, and decrypting said hashed version of said particular data  
19 random key at the first station using said particular data random key;

20       and then executing at least one additional exchange in said plurality of exchanges,

21       where

22       said at least one additional exchange includes sending an additional message from the  
23 first station to the second station carrying a next data random symmetric key from  
24 said sub-array the plurality of intermediate data random keys associated with said

25                   request, encrypted using a data random symmetric key from said sub-array  
26                   exchanged during a previously completed exchange in said plurality of  
27                   exchanges, where the second station decrypts said next data random symmetric  
28                   key and returns a responsive message carrying a hashed version of said next data  
29                   random symmetric key encrypted using said next data random symmetric key, and  
30                   decrypting at the first station said hashed version of said next data random  
31                   symmetric key using said next data random symmetric key.

1       65. (canceled).

1       66. (original) The article of claim 64, including logic executing more than one of said additional  
2       exchanges.

1       67-71. (canceled).

1       72. (currently amended) The article of claim 78 [[67]], including upon request for initiation of a  
2       communication session, logic to present to the second station a user interface for initiation of an  
3       authentication session including a compiled version of the session random symmetric encryption  
4       key and parameters for one or more conversion arrays, said user interface including a prompt for  
5       entry of said identifier of the second station the shared parameter, and at least one of said first  
6       and second shared secrets secret.

1       73-74. (canceled).

1       75. (currently amended) The article of claim 78 [[64]], including logic executing a further  
2       exchange including instructions

3                   sending a message from the first station to the second station carrying said encryption key  
4                   encrypted using a first shared secret to the second station, where the second  
5                   station returns a message carrying a hashed version of said encryption key  
6                   encrypted using said first shared secret, and decrypting said encryption key at the  
7                   first station;

8        ~~sending a message from the first station to the second station carrying said encryption key~~  
9        ~~encrypted using a second shared secret, where the second station decrypts said~~  
10      ~~encryption key, and returns a message to the first station carrying a hashed~~  
11      ~~version of the encryption key encrypted using said second shared secret; and~~  
12     sending a message from the first station to the second station carrying an authentication signal  
13     indicating success or failure of mutual authentication and establishment of the final symmetric  
14     encryption key, said authentication signal being encrypted using one of said intermediate data  
15     random symmetric keys from a previous exchange in the plurality of exchanges.

1        76. (new) A method for creating and securely distributing ephemeral random symmetric keys for  
2     use in a plurality of concurrent or spaced in time communication sessions on a communication  
3     medium between a first data processing station and a plurality of second data processing stations  
4     having access to the communication medium, in which the first station and each second station in  
5     the plurality of second stations have respective identifiers and first and second shared secrets,  
6     and for mutual authentication of the first and second stations without exchanging messages  
7     carrying said shared secrets via the communication medium, comprising:

8            receiving at the first station requests from the plurality of second stations for initiation of  
9     a communication session;

10          producing an array of session random symmetric encryption keys and plurality of sub-  
11     arrays of data random symmetric keys at the first station, where each sub-array is subordinated  
12     only to a respective session random symmetric encryption key to service a plurality of  
13     communication sessions by continuously generating, storing and obliterating the keys in the  
14     array and in the sub-arrays according to a logic at the first station; and

15          after receiving a request from a particular second station, selecting a session random  
16     symmetric encryption key from said array, and executing a plurality of exchanges of encrypted  
17     messages across said communication medium during an authentication stage of the  
18     communication session, the exchanges in the plurality of exchanges including at least one  
19     message carrying respective data random symmetric keys from the sub-array which is  
20     subordinated to the selected session random symmetric encryption key from the first station to  
21     the second station and messages respectively returning the data random symmetric keys, or their  
22     hashed equivalents, in an encrypted form from the second station to the first station, to mutually

23 authenticate the first station and the second station without exchanging the first and second  
24 shared secrets over the communication medium, and to provide one of the data random  
25 symmetric keys from the sub-array to the second station as a final symmetric encryption key for  
26 use in subsequent communications during said communication session;

27 wherein in at least one of the plurality of exchanges, the respective data random  
28 symmetric key, or its hashed equivalent, is encrypted using an intermediate data random  
29 symmetric encryption key, where the intermediate data random symmetric encryption key is one  
30 of the data random symmetric keys from said sub-array, exchanged in a previous one of the  
31 plurality of exchanges; and

32 wherein in at least one of the plurality of exchanges, the respective data random  
33 symmetric key, or its hashed equivalent, is veiled in a conversion array using the first shared  
34 secret and then, encrypted using one of the data random symmetric keys from said sub-array  
35 exchanged in a previous exchange, and

36 in at least one other of the plurality of exchanges, the respective data random symmetric  
37 key, or its hashed equivalent, is veiled in a conversion array using the second shared secret and  
38 then, encrypted using one of the data random symmetric keys from said sub-array exchanged in a  
39 previous exchange.

1 77. (new) A data processing apparatus for creating and securely distributing ephemeral random  
2 symmetric keys for use in a plurality of concurrent or spaced in time communication sessions on  
3 a communication medium between the data processing apparatus as a first station and a plurality  
4 of second data processing stations having access to the communication medium, in which the  
5 first station and each second station in the plurality of second stations have respective identifiers  
6 and first and second shared secrets, and for mutual authentication of the first and second stations  
7 without exchanging messages carrying said shared secrets via the communication medium,  
8 comprising:

9 a processor at the first station, a communication interface adapted for connection to a  
10 communication medium, and memory storing instructions for execution by the data processor,  
11 the instructions including

12 logic to receive requests via the communication interface from the plurality of second  
13 stations for initiation of a communication session;

14 logic to produce an array of session random symmetric encryption keys and plurality of  
15 sub-arrays of data random symmetric keys at the first station, where each sub-array is  
16 subordinated only to a respective session random symmetric encryption key to service a plurality  
17 of communication sessions by continuously generating, storing and obliterating the keys in the  
18 array and in the sub-arrays; and

19 logic to select, after receiving a request from a particular second station, a session random  
20 symmetric encryption key from said array, and to execute a plurality of exchanges of encrypted  
21 messages across said communication medium during an authentication stage of the  
22 communication session, the exchanges in the plurality of exchanges including at least one  
23 message carrying respective data random symmetric keys from the sub-array which is  
24 subordinated to the selected session random symmetric encryption key from the first station to  
25 the second station and messages respectively returning the data random symmetric keys, or their  
26 hashed equivalents, in an encrypted form from the second station to the first station, to mutually  
27 authenticate the first station and the second station without exchanging the first and second  
28 shared secrets over the communication medium, and to provide one of the data random  
29 symmetric keys from the sub-array to the second station as a final symmetric encryption key for  
30 use in subsequent communications during said communication session;

31 wherein in at least one of the plurality of exchanges, the respective data random  
32 symmetric key, or its hashed equivalent, is encrypted using an intermediate data random  
33 symmetric encryption key, where the intermediate data random symmetric encryption key is one  
34 of the data random symmetric keys from said sub-array, exchanged in a previous one of the  
35 plurality of exchanges; and

36 wherein in at least one of the plurality of exchanges, the respective data random  
37 symmetric key, or its hashed equivalent, is veiled in a conversion array using the first shared  
38 secret and then, encrypted using one of the data random symmetric keys from said sub-array  
39 exchanged in a previous exchange, and

40 in at least one other of the plurality of exchanges, the respective data random symmetric  
41 key, or its hashed equivalent, is veiled in a conversion array using the second shared secret and  
42 then, encrypted using one of the data random symmetric keys from said sub-array exchanged in a  
43 previous exchange.

1        78. (new) An article of manufacture, comprising:  
2              a machine readable data storage medium having computer program instructions stored  
3              therein, for creating and securely distributing ephemeral random symmetric keys for use in a  
4              plurality of concurrent or spaced in time communication sessions on a communication medium  
5              between a first data processing station and a plurality of second data processing stations having  
6              access to the communication medium, in which the first station and each second station in the  
7              plurality of second stations have respective identifiers and first and second shared secrets, and  
8              for mutual authentication of the first and second stations without exchanging messages carrying  
9              said shared secrets via the communication medium, said instructions comprising:  
10              logic to receive at the first station requests from the plurality of second stations for  
11              initiation of a communication session;  
12              logic to produce an array of session random symmetric encryption keys and plurality of  
13              sub-arrays of data random symmetric keys at the first station, where each sub-array is  
14              subordinated only to a respective session random symmetric encryption key to service a plurality  
15              of communication sessions by continuously generating, storing and obliterating the keys in the  
16              array and in the sub-arrays; and  
17              logic to select, after receiving a request from a particular second station, a session random  
18              symmetric encryption key from said array, and to execute a plurality of exchanges of encrypted  
19              messages across said communication medium during an authentication stage of the  
20              communication session, the exchanges in the plurality of exchanges including at least one  
21              message carrying respective data random symmetric keys from the sub-array which is  
22              subordinated to the selected session random symmetric encryption key from the first station to  
23              the second station and messages respectively returning the data random symmetric keys, or their  
24              hashed equivalents, in an encrypted form from the second station to the first station, to mutually  
25              authenticate the first station and the second station without exchanging the first and second  
26              shared secrets over the communication medium, and to provide one of the data random  
27              symmetric keys from the sub-array to the second station as a final symmetric encryption key for  
28              use in subsequent communications during said communication session;  
29              wherein in at least one of the plurality of exchanges, the respective data random  
30              symmetric key, or its hashed equivalent, is encrypted using an intermediate data random  
31              symmetric encryption key, where the intermediate data random symmetric encryption key is one

32 of the data random symmetric keys from said sub-array, exchanged in a previous one of the  
33 plurality of exchanges; and

34 wherein in at least one of the plurality of exchanges, the respective data random  
35 symmetric key, or its hashed equivalent, is veiled in a conversion array using the first shared  
36 secret and then, encrypted using one of the data random symmetric keys from said sub-array  
37 exchanged in a previous exchange, and

38 in at least one other of the plurality of exchanges, the respective data random symmetric  
39 key, or its hashed equivalent, is veiled in a conversion array using the second shared secret and  
40 then, encrypted using one of the data random symmetric keys from said sub-array exchanged in a  
41 previous exchange.

///